

ON THE INDEX OF LENGTH FOUR MINIMAL ZERO-SUM SEQUENCES

CAIXIA SHEN¹, LI-MENG XIA^{†,1}, AND YUANLIN LI²

¹Faculty of Science, Jiangsu University, Zhenjiang, 212013, Jiangsu Pro., China

²Department of Mathematics, Brock University, St. Catharines, ON, Canada L2S 3A1

ABSTRACT. Let G be a finite cyclic group. Every sequence S over G can be written in the form $S = (n_1g) \cdot \dots \cdot (n_lg)$ where $g \in G$ and $n_1, \dots, n_l \in [1, \text{ord}(g)]$, and the index $\text{ind}(S)$ of S is defined to be the minimum of $(n_1 + \dots + n_l)/\text{ord}(g)$ over all possible $g \in G$ such that $\langle g \rangle = G$. A conjecture on the index of length four sequences says that every minimal zero-sum sequence of length 4 over a finite cyclic group G with $\gcd(|G|, 6) = 1$ has index 1. The conjecture was confirmed recently for the case when $|G|$ is a product of at most two prime powers. However, the general case is still open. In this paper, we make some progress towards solving the general case. Based on earlier work on this problem, we show that if $G = \langle g \rangle$ is a finite cyclic group of order $|G| = n$ such that $\gcd(n, 6) = 1$ and $S = (x_1g)(x_2g)(x_3g)(x_4g)$ is a minimal zero-sum sequence over G such that $x_1, \dots, x_4 \in [1, n-1]$ with $\gcd(n, x_1, x_2, x_3, x_4) = 1$, and $\gcd(n, x_i) > 1$ for some $i \in [1, 4]$, then $\text{ind}(S) = 1$. By using an innovative method developed in this paper, we are able to give a new (and much shorter) proof to the index conjecture for the case when $|G|$ is a product of two prime powers.

Key Words: minimal zero-sum sequence, index of sequences.

2010 Mathematics Subject Classification: 11B50, 20K01

1. INTRODUCTION

Throughout the paper, let G be an additively written finite cyclic group of order $|G| = n$. By a sequence over G we mean a finite sequence of terms from G which is unordered and repetition of terms is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ and use multiplicative notation. Thus a sequence S of length $|S| = k$ is written in the form $S = (n_1g) \cdot \dots \cdot (n_kg)$, where $n_1, \dots, n_k \in \mathbb{N}$ and $g \in G$. We call S a *zero-sum sequence* if $\sum_{j=1}^k n_jg = 0$. If S is a zero-sum sequence, but no proper nontrivial subsequence of S has sum zero, then S is called a *minimal zero-sum sequence*. Recall that the index of a sequence S over G is defined as follows.

Definition 1.1. *For a sequence over G*

$$S = (n_1g) \cdot \dots \cdot (n_kg), \quad \text{where } 1 \leq n_1, \dots, n_k \leq n,$$

[†]The corresponding author's email: xialimeng@ujs.edu.cn.

the index of S is defined by $\text{ind}(S) = \min\{\|S\|_g \mid g \in G \text{ with } \langle g \rangle = G\}$, where

$$(1.1) \quad \|S\|_g = \frac{n_1 + \cdots + n_k}{\text{ord}(g)}.$$

Clearly, S has sum zero if and only if $\text{ind}(S)$ is an integer. We note that there are also slightly different definitions of the index in the literature, but they are all equivalent (see [6, Lemma 5.1.2]).

Conjecture 1.2. *Let G be a finite cyclic group such that $\gcd(|G|, 6) = 1$. Then every minimal zero-sum sequence S over G of length $|S| = 4$ has $\text{ind}(S) = 1$.*

If S is a minimal zero-sum sequence of length $|S|$ such that $|S| \leq 3$ or $|S| \geq \lfloor \frac{n}{2} \rfloor + 2$, then $\text{ind}(S) = 1$ (see [12, 14]). In contrast to that, it was shown that for each k with $5 \leq k \leq \lfloor \frac{n}{2} \rfloor + 1$, there is a minimal zero-sum subsequence T of length $|T| = k$ with $\text{ind}(T) \geq 2$ ([11, 13]) and that the same is true for $k = 4$ and $\gcd(n, 6) \neq 1$ ([11]). The only unsolved case leads to the above conjecture.

In [10], it was proved that Conjecture 1.2 holds true if n is a prime power. Recently in [9], it was proved that Conjecture 1.2 holds for $n = p_1^\alpha \cdot p_2^\beta$ (a product of two prime powers) with the restriction that at least one n_i is co-prime to $|G|$. In a most recent paper [18], the conjecture was confirmed for the remaining situation in the case when $n = p_1^\alpha \cdot p_2^\beta$. Thus these two papers together completely settle the case when n is a product of two prime powers.

Let $S = (n_1g) \cdot \dots \cdot (n_kg)$ be a minimal zero-sum sequence over G . Then S is called reduced if $(pn_1g) \cdot \dots \cdot (pn_kg)$ is no longer a minimal zero-sum sequence for every prime factor p of n . In [17] and [19], Conjecture 1.2 was proved if the sequence S is reduced. However, the general case is still open. In the present paper, we make some progress towards solving the general case and obtain the following main result.

Theorem 1.3. *Let $G = \langle g \rangle$ be a finite cyclic group of order $|G| = n$ such that $\gcd(n, 6) = 1$. Let $S = (x_1g)(x_2g)(x_3g)(x_4g)$ be a minimal zero-sum sequence over G , where $g \in G$ with $\text{ord}(g) = n$ and $x_1, \dots, x_4 \in [1, n-1]$ with $\gcd(n, x_1, x_2, x_3, x_4) = 1$, and $\gcd(n, x_i) > 1$ for some $i \in [1, 4]$. Then $\text{ind}(S) = 1$.*

2. PRELIMINARIES

Recall that G always denotes a finite cyclic group of order $|G| = n$. Given real numbers $a, b \in \mathbb{R}$, we use $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$ to denote the set of integers between a and b . For $x \in \mathbb{Z}$, we denote by $|x|_n \in [1, n]$ the integer congruent to x modulo n . Let $S = (x_1g)(x_2g)(x_3g)(x_4g)$ be a minimal zero-sum sequence over G such that $\text{ord}(g) = n = |G|$ and $1 \leq x_1, x_2, x_3, x_4 \leq n-1$. For convenience, we set $f(x_i) := \gcd(n, x_i)$ for $i \in [1, 4]$. In what follows we always assume that $\gcd(n, x_1, x_2, x_3, x_4) = 1$, so we have $\gcd(f(x_i), f(x_j), f(x_k)) = 1$ for any three different i, j, k . The following lemma is crucial and will be used frequently in sequel.

According to the assumption of Theorem 1.3, the order n of group G is not a prime number (since $1 < \gcd(n, x_i) \leq n-1 < n$ for some $i \in [1, 4]$). In what follows, we may always assume that n is an arbitrary positive integer such that $\gcd(n, 6) = 1$ and n is not a prime number unless state otherwise.

Lemma 2.1. [9, Remark 2.1]

- (1) If there exists a positive integer m such that $\gcd(n, m) = 1$ and at most one $|mx_i| < \frac{n}{2}$ (or, similarly, at most one $|mx_i| > \frac{n}{2}$), then $\text{ind}(S) = 1$.
- (2) If there exists a positive integer m such that $\gcd(n, m) = 1$ and $|mx_1|_n + |mx_2|_n + |mx_3|_n + |mx_4|_n = 3n$, then $\text{ind}(S) = 1$.

Denote by $U(n)$ the unit group of n , i.e. $U(n) = \{k \in \mathbb{N} | 1 \leq k \leq n-1, \gcd(k, n) = 1\}$. Thus $|U(n)| = \varphi(n)$ where φ is the Euler φ -function. We note that for any $y \in U(n)$ $\text{ind}(S) = \text{ind}(yS)$ where $yS = (|yx_1|_n g)(|yx_2|_n g)(|yx_3|_n g)(|yx_4|_n g)$.

Lemma 2.2. Let p be a prime factor of n and $\alpha = \frac{n}{p}$. Then for any $1 \leq v < n$ there exist elements $1 + k\alpha, 1 + j\alpha \in U(n)$ such that $|v + k\alpha|_n < \frac{n}{2}$ and $|v + j\alpha|_n > \frac{n}{2}$. Moreover, if $\gcd(v, p) = 1$, then there exists $y = 1 + t\alpha \in U(n)$ such that $|yv|_n < \frac{n}{2}$.

Proof. If $y = 1 + t\alpha \notin U(n)$, then there exists prime factor $q | \gcd(n, y)$. If $q \neq p$, we have $q | \alpha$, and thus $q | \gcd(y, \alpha) = 1$, a contradiction. We infer that $p | y$ and $\gcd(p, \alpha) = 1$. It is easy to check that at most one $t < p$ such that $y = 1 + t\alpha \notin U(n)$. So we may assume that for some t_0 , all $p-1$ terms $|1 + t_0\alpha|_n, |1 + (t_0+1)\alpha|_n, \dots, |1 + (t_0+p-2)\alpha|_n$ are in $U(n)$. If all the corresponding terms $|v + t\alpha|_n$ with $t_0 \leq t \leq t_0 + p-2$ stand in the same side of $\frac{n}{2}$, then without loss of generality, we may assume that all these terms $|v + t\alpha|_n < \frac{n}{2}$, where $t_0 \leq t \leq t_0 + p-2$. Since $(v + (t+1)\alpha) - (v + t\alpha) = \alpha < n/4$ ($t_0 \leq t \leq p-2$), we conclude that any two consecutive terms $(v + (t+1)\alpha)$ and $(v + t\alpha)$ fall into the same interval $[n\lfloor \frac{v+t\alpha}{n} \rfloor, n\lfloor \frac{v+t\alpha}{n} \rfloor + \frac{n}{2}]$. Thus all the above terms fall into the same interval, so we have $b = v + t_0\alpha < v + (t_0+1)\alpha < \dots < v + (t_0+p-2)\alpha < b + \frac{n}{2}$. Hence we infer that $(p-2)\alpha < \frac{n}{2}$, which implies that $p < 4$, giving a contradiction as $\gcd(n, 6) = 1$ and $p | n$. Thus the first statement holds.

Next assume that $\gcd(v, p) = 1$. We note that if $0 \leq t_1 \neq t_2 \leq p-1$, then $|v(1 + t_1\alpha)|_n \neq |v(1 + t_2\alpha)|_n$. Thus as a set $\{|v|_n, |v(1 + \alpha)|_n, \dots, |v(1 + (p-1)\alpha)|_n\} = \{|v|_n, |v + \alpha|_n, \dots, |v + (p-1)\alpha|_n\}$. As above, we can prove that there exists $y = 1 + t\alpha \in U(n)$ such that $|yv|_n < \frac{n}{2}$. \square

Remark 2.3. We note that if $p^2 | n$, then $y = 1 + t\alpha \in U(n)$ for any $t \in [0, p-1]$. If $p | n$ and $p^2 \nmid n$, then $\gcd(p, \alpha) = 1$, and so there is a unique $t \in [0, p-1]$ such that $y = 1 + t\alpha \notin U(n)$. In particular, if $v \in [1, n-1]$ and $p | v$, then $|yv|_n = v$ for any $y = 1 + t\alpha$.

Corollary 2.4. If $p^s | \beta < n$, $p^{s+1} \nmid \beta$ and $p^{s+1} | n$, then there exists $y = 1 + \frac{tn}{p^{s+1}} \in U(n)$ (with $0 \leq t < p$) such that $|y\beta|_n < \frac{n}{2}$.

Proof. Let $\beta_1 = \frac{\beta}{p^s}$, $n_1 = \frac{n}{p^s}$ and $\alpha = \frac{n_1}{p} = \frac{n}{p^{s+1}}$. Then $1 \leq \beta_1 < n_1$ and $\gcd(\beta_1, p) = 1$. By Lemma 2.2, there exists $y = 1 + t\alpha \in U(n_1) \subseteq U(n)$ such that $|y\beta_1|_{n_1} < \frac{n_1}{2}$. Thus $|y\beta|_n = |y\beta_1 p^s|_n = p^s |y\beta_1|_{n_1} < p^s \frac{n_1}{2} = \frac{n}{2}$ as desired. \square

Lemma 2.5. *If $f(x_1) = f(x_2) = d > 1$, then $\text{ind}(S) = 1$.*

Proof. We first show that there exists $u \in U(n)$ such that $|ux_1|_n < \frac{n}{2}$ and $|ux_2|_n < \frac{n}{2}$. By multiplying S by a unit, we may assume that $x_1 = d$ and $x_2 = n - kd$, where $k \in U(n)$. If $kd > \frac{n}{2}$, then we are done. So we may assume that $kd < \frac{n}{2}$. Since S is a minimal zero-sum sequence, we conclude that $k \neq 1$, so $x_1 = d < \frac{n}{2k} \leq \frac{n}{4}$. If $kd > \frac{n}{4}$, then $2x_1 = 2d \leq kd < \frac{n}{2}$ and $\frac{n}{2} < 2kd < n$. Let $u = 2$. Then we get $|ux_1|_n < \frac{n}{2}$ and $|ux_2|_n < \frac{n}{2}$ as desired. If $kd < \frac{n}{4}$, then there exists s such that $2^s x_1 < \frac{n}{4} \leq 2^s kd < \frac{n}{2}$. Let $u = 2^{s+1}$. Then $|ux_1|_n < \frac{n}{2}$ and $|ux_2|_n < \frac{n}{2}$ as desired.

Next we may assume that $x_1 < \frac{n}{2}$ and $x_2 < \frac{n}{2}$. Let p be a prime factor of d and $\alpha = \frac{n}{p}$. Then $\gcd(p, x_3) = 1$. By Lemma 2.2, there exists $y = 1 + j\alpha \in U(n)$ such that $|yx_3|_n < \frac{n}{2}$. Since y fixes x_1 and x_2 (i.e. $|yx_1|_n = x_1$ and $|yx_2|_n = x_2$), by (1) of Lemma 2.1, we have $\text{ind}(S) = \text{ind}(yS) = 1$. \square

Next we assume that n has at least three prime factors. Then for every prime $p|n$, we have $p \geq 11$ or $\alpha = \frac{n}{p} \geq 55$. This estimate for α will be used in Lemmas 2.6-2.7, and then in Lemmas 2.9-2.10.

Lemma 2.6. *If $f(x_1) = 7$, $\gcd(f(x_1), f(x_2)) = \gcd(f(x_1), f(x_3)) = \gcd(f(x_1), f(x_4)) = 1$ and $7^2 \nmid n$, then $\text{ind}(S) = 1$.*

Proof. Let $\alpha = \frac{n}{7}$. As noted in Remark 2.3 there exist exactly six $t \in [0, 6]$ such that $y = 1 + t\alpha \in U(n)$. By multiplying S with a suitable unit, we may assume that $x_1 = \frac{n-7}{2}$. Note that $|yx_1|_n = x_1 < \frac{n}{2}$ for any $y = 1 + t\alpha \in U(n)$. We may also assume that exactly one of $|yx_2|_n, |yx_3|_n, |yx_4|_n$ is less than $\frac{n}{2}$. For otherwise, it follows from Lemma 2.1 that $\text{ind}(S) = 1$, and we are done.

We claim that there exist at most two elements $y = 1 + t\alpha \in U(n)$ such that both $|yx_3|_n > \frac{n}{2}$ and $|yx_4|_n > \frac{n}{2}$. For otherwise, we infer that either at least five $|yx_3|_n$ or at least five $|y'x_4|_n$ are greater than $\frac{n}{2}$. As in the proof of Lemma 2.2, this implies that $(5-1)\alpha < \frac{n}{2}$, so $\frac{4}{7}n < \frac{n}{2}$, giving a contradiction.

If there exists at most one element $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n > \frac{n}{2}$ and $|yx_4|_n > \frac{n}{2}$, then there exist at least five elements $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n$ and $|yx_4|_n$ stand in different sides of $\frac{n}{2}$. Hence by the assumption that exactly one of $|yx_2|_n, |yx_3|_n, |yx_4|_n$ is less than $\frac{n}{2}$, we conclude that $|yx_2|_n > \frac{n}{2}$ for all these five y . As above, we have $(5-1)\alpha < \frac{n}{2}$, giving a contradiction again.

Next we may assume there exist exactly two elements $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n > \frac{n}{2}$ and $|yx_4|_n > \frac{n}{2}$. Thus exactly four $|yx_3|_n > \frac{n}{2}$ and exactly four $|y'x_4|_n > \frac{n}{2}$. A similar discussion on x_2 and x_3 shows that exactly four $|y''x_2|_n > \frac{n}{2}$.

Since $|yx_1|_n = x_1$ for any $y = 1 + t\alpha \in U(n)$ ($t \in [0, 6]$), we have

$$\begin{aligned}
 M &= \sum_{\substack{y=1+t\alpha \in U(n) \\ t \in [0,6]}} \sum_{i=1}^4 |yx_i|_n = \sum_{i=1}^4 \sum_{\substack{y=1+t\alpha \in U(n) \\ t \in [0,6]}} |yx_i|_n \\
 &\geq 6 \times \frac{n-7}{2} \\
 &\quad + (x'_2 + (x'_2 + \alpha) + (x'_2 + 3\alpha) + (x'_2 + 4\alpha) + (x'_2 + 5\alpha) + (x'_2 + 6\alpha)) \\
 &\quad + (x'_3 + (x'_3 + \alpha) + (x'_3 + 3\alpha) + (x'_3 + 4\alpha) + (x'_3 + 5\alpha) + (x'_3 + 6\alpha)) \\
 &\quad + (x'_4 + (x'_4 + \alpha) + (x'_4 + 3\alpha) + (x'_4 + 4\alpha) + (x'_4 + 5\alpha) + (x'_4 + 6\alpha)) \\
 &= 3n - 21 + 6x'_2 + 6x'_3 + 6x'_4 + 57\alpha,
 \end{aligned}$$

where $|yx_i|_n = x'_i + t_i\alpha$ and $x'_i < \alpha$.

Since there are exactly four y such that $|yx_i|_n > \frac{n}{2}$ for $i \in [2, 4]$, we conclude that $x'_i + 3\alpha > \frac{n}{2}$, which implies that $x'_i > \frac{\alpha}{2}$ for $i \in [2, 4]$. Now we infer that

$$M > 3n - 21 + 66\alpha = 12n + 3(\alpha - 7) > 12n,$$

and thus there exists at least one $y = 1 + t\alpha$ such that $|yx_1|_n + |yx_2|_n + |yx_3|_n + |yx_4|_n = 3n$. By Lemma 2.1, we get $\text{ind}(S) = 1$ as desired. \square

Lemma 2.7. *If $f(x_1) = 5$, $\gcd(f(x_1), f(x_2)) = \gcd(f(x_1), f(x_3)) = \gcd(f(x_1), f(x_4)) = 1$ and $5^2 \nmid n$, then $\text{ind}(S) = 1$.*

Proof. The proof is similar to that of the above lemma. \square

Lemma 2.8. *If $\gcd(f(x_1), f(x_2)) = d > 1$, then $\text{ind}(S) = 1$.*

Proof. If $f(x_1) = f(x_2) = d$, the result follows from Lemma 2.5. So we may assume that $x_1 = f(x_1) > d$. Note that $x_1 = f(x_1) < \frac{n}{2}$.

Since $x_1 > d$, there must exist a prime p and a non-negative integer s such that $p^s | x_2$, $p^{s+1} \nmid x_2$ and $p^{s+1} | x_1$ (in fact, we may choose p to be any prime factor of $\frac{x_1}{d}$). Let $\alpha = \frac{n}{p^{s+1}}$. By Corollary 2.4, there exists $y = 1 + k\alpha \in U(n)$ such that $|yx_2|_n < \frac{n}{2}$. We note that $|yx_1|_n = x_1 < \frac{n}{2}$.

By multiplying S by such y , we may assume that $x_1 < \frac{n}{2}$ and $x_2 < \frac{n}{2}$. Choose a prime p such that $p | d$ and let $\alpha' = \frac{n}{p}$. Since $\gcd(d, x_3) = 1$, $\gcd(p, x_3) = 1$, so it follows from Lemma 2.2 that there exists $y_1 = 1 + k_1\alpha' \in U(n)$ such that $|y_1x_3|_n < \frac{n}{2}$. Since y_1 fixes both x_1 and x_2 , it follows from Lemma 2.1 that $\text{ind}(S) = 1$. \square

Lemma 2.9. *If $f(x_1) > 1$, $f(x_2) > 1$ and $\gcd(f(x_1), f(x_2)) = 1$, then $\text{ind}(S) = 1$.*

Proof. First we assume that $x_1 = f(x_1) < \frac{n}{2}$. Let p and q be the largest primes such that $p | f(x_1)$ and $q | f(x_2)$, and set $\alpha = \frac{n}{p}$. Without loss of generality, we may assume that $p > q$. In view of Lemma 2.8, we may also assume that $\gcd(f(x_1), f(x_i)) = 1$ for all $i \in [2, 4]$.

Next, since $\gcd(x_1, q) = 1$, we may assume that $x_3 = w_1x_1 + v_1q$ and $x_4 = w_2x_1 + v_2q$ where $\gcd(x_1, v_i) = 1$ for all $i \in [1, 2]$. As in Lemma 2.2, there exists at most one $t \in [0, p-1]$ such that $y = 1 + t\alpha \notin U(n)$. If $(1 + t\alpha)x_3 = (1 + s\alpha)x_3 \pmod{n}$, then $n|(t-s)\alpha v_1q$, and thus $p|(t-s)$ (as $\gcd(p, v_1q) = 1$), so $t = s$. A similar result holds for x_4 .

If there doesn't exist any y such that $|yx_3|_n < \frac{n}{2}$ and $|yx_4|_n < \frac{n}{2}$ and there exist at least three y such that both $|yx_3|_n > \frac{n}{2}$ and $|yx_4|_n > \frac{n}{2}$, then there exist at least $\frac{p-1}{2} + 2$ many y such that $|yx_3|_n > \frac{n}{2}$ or $|yx_4|_n > \frac{n}{2}$. This implies that $\frac{p}{2} > \frac{p-1}{2} + 2 - 1 = \frac{p+1}{2}$, giving a contradiction. Thus, either we can find $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n < \frac{n}{2}$ and $|yx_4|_n < \frac{n}{2}$, or there exist at least $p-3$ many $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n$ and $|yx_4|_n$ stand in different sides of $\frac{n}{2}$ for each y . For the former case, as before we have $\text{ind}(S) = 1$ by Lemma 2.1.

Next we consider the latter case. If $p \geq 11$, we can find $y = 1 + t\alpha \in U(n)$ such that $|yx_2|_n < \frac{n}{2}$. For otherwise, for these $p-3$ many y we have $|yx_2|_n > \frac{n}{2}$. As before, we infer that $\frac{p}{2} > p-4$ and thus $p < 8$, giving a contradiction.

Now assume that $p = 7$. Since $\gcd(f(x_1), f(x_2)) = 1$, we conclude that $f(x_1) = 7^\lambda$ and $f(x_2) = 5^\mu$. If $7^2|n$, then either we can find $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n < \frac{n}{2}$ and $|yx_4|_n < \frac{n}{2}$, or, as before, there exist at least 6 elements $y = 1 + t\alpha \in U(n)$ such that $|yx_3|_n$ and $|yx_4|_n$ stand in different sides of $\frac{n}{2}$. For the latter case, we can find $y \in U(n)$ such that at least two of $|yx_2|_n < \frac{n}{2}$, $|yx_3|_n < \frac{n}{2}$ and $|yx_4|_n < \frac{n}{2}$ hold. Thus in both cases we have $\text{ind}(S) = 1$ by Lemma 2.1. Finally, if $7^2 \nmid n$, by Lemma 2.6, we have $\text{ind}(S) = 1$. This completes the proof. \square

Lemma 2.10. *If $f(x_1) = d > 1$ and $f(x_2) = f(x_3) = f(x_4) = 1$ (i.e. x_2, x_3, x_4 are co-prime to n), then $\text{ind}(S) = 1$.*

Proof. Let p be the largest prime factor of $f(x_1)$ and $\alpha = \frac{n}{p}$. Since x_2, x_3, x_4 are co-prime to n (hence they are co-prime to p), we may assume that $x_i = w_ip + v_i$ for $i \in [2, 4]$, where $v_i \in [1, p-1]$. Again, we can show that $(1 + t\alpha)x_i = (1 + s\alpha)x_i \pmod{n}$ for any $i \in [2, 4]$ if and only if $t = s$.

If $p \geq 11$ or $p^2|n$, a proof similar to that of Lemma 2.9 shows that $\text{ind}(S) = 1$. If $p \leq 7$, $f(x_1) = p \in \{5, 7\}$ and $p^2 \nmid n$, by Lemmas 2.6 and 2.7, we get $\text{ind}(S) = 1$ as desired. Finally, we consider the last case when $p = 7$, $p^2 \nmid n$ and $f(x_1) = 5 \cdot 7 = 35$. Since n has at least three different prime factors and $\alpha = \frac{n}{7} \geq 55$. As in the proof of Lemma 2.6, we may assume that $x_1 = \frac{n-35}{2}$ and we can reduce to the only case that there are exactly four $y = 1 + t\alpha \in U(n)$ such that $|yx_i|_n > \frac{n}{2}$ for each $i \in [2, 4]$. As before, we can estimate the sum M as follows:

$$\begin{aligned}
 M &= \sum_{\substack{y=1+t\alpha \in U(n) \\ t \in [0,6]}} \sum_{i=1}^4 |yx_i|_n = \sum_{i=1}^4 \sum_{\substack{y=1+t\alpha \in U(n) \\ t \in [0,6]}} |yx_i|_n \\
 &> 3n - 105 + 66\alpha = 12n + 3(\alpha - 35) > 12n.
 \end{aligned}$$

Thus there exists at least one $y = 1+t\alpha \in U(n)$ such that $|yx_1|_n + |yx_2|_n + |yx_3|_n + |yx_4|_n = 3n$. By Lemma 2.1, we get $\text{ind}(S) = 1$ as desired. \square

3. PROOF OF MAIN RESULT

As mentioned early, in [18] the authors settled the remaining case when $|G|$ is a product of two prime powers. However, the proof is quite long. By applying an innovative method developed in this paper, we are able to give a new and very short proof for the above mentioned case. This together with [9] provides a complete solution to the index conjecture for the product of two prime-power case.

Theorem 3.1. *Let $G = \langle g \rangle$ be a finite cyclic group of order $|G| = n$ such that $\gcd(n, 6) = 1$ and $n = p^\beta q^\gamma$ is a product of two different prime powers. If $S = (x_1g)(x_2g)(x_3g)(x_4g)$ is any minimal zero-sum sequence over G , then $\text{ind}(S) = 1$.*

Proof. In view of [9, Theorem 1.3], we may assume $f(x_i) > 1$ for each $i \in [1, 4]$. We may also assume that $\gcd(f(x_1), f(x_2), f(x_3), f(x_4)) = 1$, $p \mid \gcd(f(x_1), f(x_2))$ and $q \mid \gcd(f(x_3), f(x_4))$. Thus we get that $f(x_1) = p^{s_1}$, $f(x_2) = p^{s_2}$, $f(x_3) = q^{s_3}$, and $f(x_4) = q^{s_4}$ with $s_i \geq 1$, $i \in [1, 4]$. Without loss of generality, we may assume that $x_1 = f(x_1) < \frac{n}{2}$ and $f(x_1) \geq f(x_2)$ (i.e. $s_1 \geq s_2$). We divide the proof into two cases.

Case 1. $f(x_1) = f(x_2) = \gcd(f(x_1), f(x_2)) > 1$. As in Lemma 2.5, we can find $u \in U(n)$ such that $|ux_1|_n < \frac{n}{2}$ and $|ux_2|_n < \frac{n}{2}$. Since $\gcd(|ux_3|_n, p) = 1$, by Lemma 2.2, there exists $y = 1 + t\frac{n}{p} \in U(n)$ such that $|yux_3|_n < \frac{n}{2}$. Note also that $|yux_i|_n = |ux_i|_n < \frac{n}{2}$ for all $i \in [1, 2]$. So it follows from Lemma 2.1 that $\text{ind}(S) = 1$.

Case 2. $f(x_1) > f(x_2) = p^{s_2}$. Note that $p^{s_2} \mid f(x_2)$, $p^{s_2+1} \nmid f(x_2)$ and $p^{s_2+1} \mid f(x_1)$. By Corollary 2.4, there exist $u = 1 + t\alpha \in U(n)$ with $\alpha = \frac{n}{p^{s_2+1}}$ such that $|ux_2|_n < \frac{n}{2}$. Note also that $|ux_1|_n = x_1 < \frac{n}{2}$. As in Case 1, we can find $y = 1 + t\frac{n}{p} \in U(n)$ such that $|yux_i|_n < \frac{n}{2}$ for all $i \in [1, 3]$. Therefore, $\text{ind}(S) = 1$ as desired. \square

Proof of Theorem 1.3.

If n has at most two distinct prime factors, the result follows immediately from [9] and Theorem 3.1. So we need only consider the case when n has at least three distinct prime factors. Assume that $x_1 = f(x_1) = d > 1$ and n has at least three distinct prime factors. We divide the proof into the following two cases:

Case 1. At least one $\gcd(f(x_1), f(x_i)) > 1$ for $i \in [2, 4]$. Without loss of generality, we may assume that $\gcd(f(x_1), f(x_2)) > 1$. It follows from Lemma 2.8 that $\text{ind}(S) = 1$.

Case 2. All $\gcd(f(x_1), f(x_i)) = 1$ for $i \in [2, 4]$. We divide the proof into two subcases.

Subcase 2.1. At least one $f(x_i) > 1$ for $i \in [2, 4]$. Without loss of generality, we may assume that $f(x_2) > 1$. The result follows from Lemma 2.9.

Subcase 2.2. $f(x_2) = f(x_3) = f(x_4) = 1$. The result follows from Lemma 2.10. \square

ACKNOWLEDGEMENTS

We would like to thank the referee for valuable suggestions which helped in improving the readability of the paper. A part of research was carried out during a visit by the third author to Jiangsu University. He would like to gratefully acknowledge the kind hospitality from the host institution. This research was supported in part by the NNSF of China (Grant No. 11001110, 11271131) and a Discovery Grant from the Natural Science and Engineering Research Council of Canada.

REFERENCES

- [1] S.T. Chapman, and W.W Smith, *A characterization of minimal zero-sequences of index one in finite cyclic groups*, Integers 5 (1) (2005), Paper A27, 5p.
- [2] W. Gao, *Zero sums in finite cyclic groups*, Integers 0 (2000), Paper A14, 9p.
- [3] W. Gao and A. Geroldinger, *On products of k atoms*, Monatsh. Math. 156 (2009), 141-157.
- [4] W. Gao, Y. Li, J. Peng, P. Pyley and G. Wang *On the index of sequences over cyclic groups* (English), Acta Arith. 148 (2) (2011), 119-134.
- [5] A. Geroldinger, *On non-unique factorizations into irreducible elements. II*, Number Theory, Vol II Budapest 1987, Colloquia Mathematica Societatis Janos Bolyai, vol. 51, North Holland, 1990, 723-757.
- [6] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1-86.
- [7] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations*. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, Vol. 278, Chapman & Hall/CRC, 2006.
- [8] J. Peng and Y. Li, *Minimal zero-sum sequences of length five over finite cyclic groups*, Ars Combinatoria 112 (2013), 373-384.
- [9] Y. Li and J. Peng, *Minimal zero-sum sequences of length four over finite cyclic groups II*, International Journal of Number Theory 9 (2013), 845-866.
- [10] Y. Li, C. Pyley, P. Yuan and X. Zeng, *Minimal zero sum sequences of length four over finite cyclic groups*, Journal of Number Theory 130 (2010), 2033-2048.
- [11] V. Ponomarenko, *Minimal zero sequences of finite cyclic groups*, Integers 4 (2004), Paper A24, 6p.
- [12] S. Savchev and F. Chen, *Long zero-free sequences in finite cyclic groups*, Discrete Math. 307 (2007), 2671-2679.
- [13] X. Xia and P. Yuan, *Indexes of insplitable minimal zero-sum sequences of length $l(C_n) - 1$* , Discrete Math. 310 (2010), 1127-1133.
- [14] P. Yuan, *On the index of minimal zero-sum sequences over finite cyclic groups*, J. Combin. Theory Ser. A114 (2007), 1545-1551.

- [15] P. Yuan and X. Zeng, *Indexes of long zero-sum free sequences over cyclic groups*, Eur. J. Comb. 32 (2011), 1213-1221.
- [16] D. J. Gryniewicz, *Structural Additive Theory, Developments in Mathematics*, Springer, 2013.
- [17] L. Xia, *On the index-conjecture on length four minimal zero-sum sequences*, International Journal of Number Theory, Vol. 9, No. 6 (2013) 1505-1528. Doi: 10.1142/S1793042113500401.
- [18] L. Xia and C. Shen, *Minimal zero-sum sequences of length four over cyclic group with order $n = p^\alpha q^\beta$* , Journal of Number Theory 133 (2013) pp. 4047-4068.
- [19] Caixia Shen, Li-meng Xia, *On the index-conjecture on length four minimal zero-sum sequences II*, International Journal of Number Theory, to appear, DOI: 10.1142/S179304211350111X.